(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 952 511 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
27.10.1999 Bulletin 1999/43

(51) Int. Cl.[6]: **G06F 1/00**

(21) Application number: **99104946.1**

(22) Date of filing: **12.03.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **23.04.1998 US 66505**

(71) Applicant:
Siemens Information and Communication Networks Inc.
Boca Raton, FL 33487 (US)

(72) Inventors:
- **Shaffer, Shmuel**
  Palo Alto, CA 94301 (US)
- **Beyda, William J.**
  Cupertino, CA 95014 (US)

(74) Representative: **Allen, Derek**
Siemens Group Services Limited,
Intellectual Property Department,
Siemens House,
Oldbury
Bracknell, Berkshire RG12 8FZ (GB)

(54) Method and system for providing data security and protection against unauthorised telephonic access

(57) A method and system for providing security for a computing device include resolving, conflicts between a password-protected screen saver and communication notification capabilities by selectively enabling access to specific communications when the computing device is in a locked mode. The screen saver of the computing device is configured to switch the device from a normal operative mode to a locked mode in response to detection of a preset condition, such as the expiration of an idle-time timer. The computing device then remains in the locked mode until a preset authorization condition is recognized, e.g., entering a password. However, with the computing device in the locked mode, a subset of communication access capabilities is enabled. Specifically, notification of incoming communications is enabled. Preferably, connectivity for select types of outgoing calls is also enabled, e.g., connectivity for emergency calls. In the preferred embodiment, the conflicts are resolved by integrating the screen saver with communication access capabilities in a single software package. Also in the preferred embodiment, the communication access capabilities are provided by a telephony over LAN application and a switch to the locked mode is disabled during communication sessions involving the computing device.

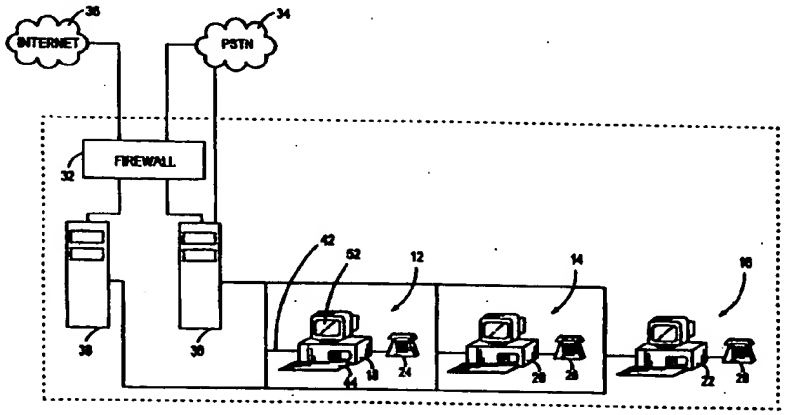

FIG. 1

EP 0 952 511 A2

Description

BACKGROUND OF THE INVENTION

[0001] The invention relates generally to methods and systems for limiting access to capabilities of a computer and more particularly to methods and systems for protecting data and communications capabilities of a computer that is connected to a network that handles message exchanges.

DESCRIPTION OF THE RELATED ART

[0002] There are a number of mechanisms available for providing security within a network of computers, such as a local area network (LAN) or wide area network (WAN). A firewall is an electronic barrier that provides network security by determining how outside users and servers access resources of the network via dial-up lines or another network. For example, a password may be necessary to gain access to network resources. With added sophistication, a dial-back tool may be utilized as a component of a firewall. When a dial-in user is identified, the network terminates the connection and dials-back the user at a predetermined number, ensuring that a remote computer is indeed the authorized computer for accessing the network.

[0003] Still at the network level, user security mechanisms determine how, when, and where network users can gain access to the network resources. Within an enterprise, there are often restrictions regarding which persons can access various types of information and various network resources. For example, information relating to a particular project may be restricted to management and persons assigned to the project. Access to sensitive data may be restricted by user authentication (e.g., a password or a biometric technique such as a voiceprint authentication) or by device authentication in which only designated computers may gain access, so that the system need only distinguish the computers.

[0004] There are also security concerns at the individual computer level. Confidential information may be apparent on the monitor screen of an unattended computer or may be readily accessible by unauthorized individuals using another person's computer. A departing employee may gain access to marketing information and developing designs and concepts by using the computer of another employee to access the internally stored data of the computer or to access network data having computer-specific restriction requirements.

[0005] A security mechanism that is available at the computer level is a time-based screen saver that is password protected. If a computer remains idle for a selectable period of time, the resources of the computer are locked and the potentially sensitive information on the screen is deleted. In a screen saver mode, the screen may be blanked or may have a sequencing image that does not include sensitive material. Many corporations require the use of a password-protected screen saver to provide security.

[0006] In the corporate environment, there is also a trend to incorporate telephony within the data network. For example, telephony over LAN (TOL) applications allow the handling of telephone calls via a computer. A TOL application handles both video and audio information. When an incoming call is detected, a notification is presented on the computer screen of the target computer. The notification is run in a minimize mode, or in the system tray of some operating systems.

[0007] A concern is that the use of a TOL application is inconsistent with screen saver applications. As noted above, if a computer remains idle for a selected period of time, the resources of the computer may be automatically locked to ensure data security. However, this locked mode disables the TOL application. Consequently, a person may not receive notification of an incoming call. Optionally, the TOL application may be dominant, so that an incoming call will override the screen saver. In this case, the security provided by the screen saver application is compromised. A person intent on accessing data of an unoccupied computer can unlock the resources of the computer merely by calling the computer from a second computer in the same area. As another alternative, the screen saver application may be dominant, so that the input of a password is required in order to access an incoming call. While this alternative ensures that an unattended computer is not unlocked by an incoming call, it requires that a user quickly enter the password into a computer that is the target of a business call and that is in the locked mode, or the business call will be missed.

[0008] Another concern with the use of a TOL application with a password-protected screen saver application is that there are added risks in emergency conditions. In an emergency, a password must be entered into a computer before a reporting call can be made (e.g., call "911"). At best, this will slow down the process of reporting the situation. At worst, the password requirement will prevent the reporting call from being completed, since the person aware of the situation may not be near a computer for which he or she is aware of the appropriate password.

[0009] What is needed is a method and system that accommodate the combination of an access-restricted application and a communications-enabling application within a single computing device.

SUMMARY OF THE INVENTION

[0010] A method and system of maintaining security for a computing device connected to a network include resolving conflicts between communication access capability and a screen saver by selectively enabling access to communications when the computing device is in a locked mode. In the preferred embodiment, the communications are incoming telephone calls, but the

method and system may be used in other messaging applications, e.g., email applications. Also in the preferred embodiment, the conflicts are resolved by integrating the screen saver and the communication access capabilities in a single software package. In a less preferred embodiment, the conflicts are resolved by utilizing an arbitrating application to allow selective "break through" of a conventional screen saver application.

[0011] In a first step, the computing device is configured to switch the device from a normal operative mode to a locked mode in response to detection of a preset condition, such as the expiration of an idle-time timer. Thus, if the computer remains idle for a preselected period of time, a computing device is switched to a locked mode that establishes a security condition with respect to data access capabilities and communication access capabilities. The computing device remains in the locked mode until a preset authorization condition is recognized. This preset authorization condition may be the entering of a password, but other authentication procedures may be required, e.g., a voiceprint recognition.

[0012] In the preferred embodiment, telephone activity prevents the preset condition from being established. Thus, the idle-time timer cannot expire while the user is engaged in a telephone call.

[0013] The method and system also include enabling notification at the computing device when an incoming communication is directed to the device. In a telephony over LAN (TOL) situation, the TOL application may be allowed to open in a minimized state upon detection of an incoming telephone call. However, only a subset of the communication access capabilities are unlocked, while data access capabilities and a second subset of communication access capabilities remain in the locked mode. For example, maximizing the state of the screen notification may not be permitted and the user may be unable to open any other windows. Thus, the call can be answered, but the computing device is locked in the TOL window.

[0014] If the user has not entered the preset authorization condition (e.g., input the correct password), the computing device returns to an apparently locked mode upon completion of the incoming call. That is, the incoming call does not compromise either the data access security or the communication access security of the screen saver, other than for handling incoming communications.

[0015] In the preferred embodiment, the subset of communication access capabilities that is enabled when the computing device is in the locked mode includes the ability to initiate specified types of outgoing calls. Preferably, emergency numbers may be recognized. For example, a "911" call may be initiated without entering a password. The screen saver application preferably remains in the locked mode during the emergency call. In addition to a "911" call, internal emergency numbers may be recognized when entered in a screen saver input line. Optionally, other internal numbers may be recognized, while maintaining the security of the communication access capabilities with respect to initiating calls that are external to a particular TOL environment.

[0016] The computing device includes the screen saver capability and the communications capability. As previously noted, the two capabilities are preferably integrated into a single program, but may be separate programs that are controlled in common. The screen saver capability switches the computing device to a locked mode that establishes the security conditions for disabling data access and restricting communication access. The computing device includes a mechanism for recognizing a predefined authorization sequence that unlocks the device from the security condition. However, when the computing device is in the security condition, a limited number of communication access capabilities are enabled. The enabled communication access capabilities include the ability to handle incoming communications and, optionally, the ability to initiate certain types of outgoing communications, e.g., emergency calls.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017]

Fig. 1 is a schematic view of a network of computing devices for handling incoming and outgoing communications in accordance with the invention.
Fig. 2 is a schematic view of components of the computing device of Fig. 1.
Fig. 3 is a process flow of steps for implementing a security system in accordance with the invention.

DETAILED DESCRIPTION

[0018] With reference to Fig. 1, a topology of a network 10 having security for protecting data and resources from unauthorized access is shown as having three computing devices 12, 14 and 16 that each include a computer 18, 20 and 22 and a telephone 24, 26 and 28. The telephones are not critical to the invention, since a telephony over LAN (TOL) capability may be achieved by using the resources of the computers (e.g., sound cards and internal or external speakers). Preferably, the computing devices 12-16 are telephony clients that handle incoming and outgoing telephone calls via a telecommunications server 30. The telecommunications server 30 is shown as being connected to the public switched telephone network (PSTN) 34, allowing it to convert the gateway function of converting between circuit switched (PSTN) and packet switched (TOL) voice. The telecommunications server is also linked to a firewall 32 and the global communications network referred to as the Internet 36. As is well known in the art, a firewall provides an electronic barrier to limit access to network data and resources from outside the

network. Thus, voice and video calls are connected to the network directly to the telecommunications server (with the server providing any desired security), while data calls might be connected back through the firewall via a modem to provide the desired data security.

[0019] The computing devices 12, 14 and 16 are also connected to a message server 38. The message server may handle one or more types of messages that are stored for access by the computing devices. For example, the server 38 may store email messages or fax messages. While the method to be described below is preferably applied to selectively breaking through a screen saver capability as a result of detecting an incoming telephone call, the invention may be used in other messaging applications, such as email and facsimile message exchanges associated with the server 38.

[0020] Referring now to Figs. 1 and 2, relevant components of the computing device 12 are shown as including a network link 40 having an input 42 that is connected to the servers 30 and 38. The means for providing the network link is not critical to the invention. The input may be a cable connected to a wired port of the computer 18. Alternatively, wireless connections may be utilized, such as infrared transmission to a photoreceptor on the computer.

[0021] The computing device 12 includes at least one user input device 44. Typical user input devices include a computer keyboard and a computer mouse. In addition to the user input devices and the network link 40, other conventional components of the computing device 12 include a central processing unit (CPU) 46, local memory 48, video random access memory (VRAM) 50 and a computer monitor 52. As is well known in the art, the CPU 46 controls the operations of the computing device. The local memory 48 may include an internal hard disk drive and peripheral drives having fixed or replaceable storage media. Data from the CPU 46 is used to update VRAM 50 for display at the computer monitor 52, as is well known in the art.

[0022] The computing device 12 includes TOL capability 54 and screen saver capability 56. While Fig. 2 shows the TOL and the screen saver as separate applications, in the preferred embodiment the two capabilities are integrated into a single application. If the two capabilities are implemented in separate applications, an arbitrating application may be used to manage the two applications, thereby providing compatibility.

[0023] A security module 58 is shown as being connected between the user input devices 44 and the screen saver 56. The security module is software based and is similar to conventional security modules for use with screen savers, but preferably includes the additional capability of monitoring activity of the TOL, preventing the screen saver security from being triggered during a telephone call. The security module may include a timing mechanism that monitors manipulation of the user input devices 44 to detect periods of inactivity. The screen saver capability is configurable with respect to selecting a particular time period, so that the screen saver 56 switches the computing device 12 to a locked mode when the computing device is idle for a period exceeding the preselected period. That is, if there is no activity by any of the user input devices for a configurable period of time during which the user is not engaged in a call, the screen saver triggers a locked mode. In the preferred embodiment, the locked mode inhibits access to user data within the local memory 48, controls the display at the computer monitor 52, and restricts communication with the network via the network link 40.

[0024] In operation, if the user of the computing device 12 leaves the device unattended, the security module 58 detects when the preconfigured time-out period has been exceeded. The screen saver switches the computing device to the locked mode. The user data of the local memory 48 is secured by disabling access to the stored user data of the memory. More-over, any sensitive material displayed on the monitor 58 is removed. The locked mode may cause the computer monitor to be blanked or may trigger display of an image sequence. For example, the corporate logo may be displayed as continuously moving across the monitor.

[0025] While the security module 58 is shown as being connected only to the user input devices 44, typically the module is connected to other components of the computing device 12, so that switching between a normal operation mode and the locked mode is dependent upon a number of actions. For example, if there is an extended period of inactivity by the user input devices 44, but the TOL 54 indicates that the user is engaged in a lengthy telephone call, the computing device will remain in the normal operation mode. Similarly, if it is determined that the CPU 46 is engaged in complex calculations with a spreadsheet program, so that the user input devices are inactive, the computing device remains in the normal operation mode.

[0026] Alternatively, under certain conditions the screen saver 56 may trigger a switch to the locked mode prior to expiration of the time-out period, if the security module 58 has been preconfigured to provide the premature switch. As one example, a user may intentionally "park" a cursor in a preselected corner of the monitor 52 in order to immediately switch from the normal operation mode to the locked mode. As another example, a sequence of keys on the keyboard may be depressed to automatically trigger the locked mode. Thus, a user is able to immediately secure the computing device 12 when he or she leaves the area of the computing device.

[0027] One concern with prior art computing devices that include both screen saver and TOL capabilities is that there are conflicts between the purposes of the two applications. If the screen saver 56 of Fig. 2 is operated without concern for the TOL capability 54, a user will be unable to receive incoming communications or direct

outgoing communications when the computing device 12 is in the locked mode. On the other hand, if the TOL capability is implemented without regard for the security provided by the screen saver capability, security of stored data and the telecommunications capabilities is compromised merely by directing a call to the TOL client. For example, user data at the local memory may be switched from being inaccessible to being accessible merely by directing a call to the TOL client 54.

[0028] Another concern is that the screen saver 56 may slow or even block the report of an emergency condition. Typically, the switch from the locked mode to the normal operation mode requires an authentication process. The screen saver may be password protected or may require a biometric authorization, such as a voiceprint authentication. If the authorized person is available, the authentication process must be followed before an emergency is reported. If the authorized person is unavailable, another means for reporting the emergency must be utilized.

[0029] Fig. 3 is a process flow for a method of maintaining security of the computing device while resolving conflicts between the communication access capability and the screen saver. The conflicts are resolved by allowing selective "break through" of a conventional screen saver application. In step 60, the screen saver 56 of Fig. 2 is configured to define a number of operational parameters. The parameters include setting the conditions under which the computing device 12 is switched from the normal operational mode to the locked mode. This may merely be an identification of a period of idle time before the switch is executed. The configuration of the operational parameters may also include defining the authorization condition, such as the input of a particular password or the selection of a particular biometric technique, e.g., voiceprint recognition.

[0030] The configuration of operational parameters within the step 60 may also include defining particular types of calls that can be initiated when the screen saver is in the locked mode. Preferably, emergency numbers may be dialed. That is, the computing device 12 may be configured to allow dialing of "911" and internal emergency numbers. For example, "Enter password or 911 for emergencies" or a separate "emergency button" could exist on the screen saver input window to automate the dialing of the emergency number. In this manner, someone walking near the computing device could use the TOL 54 to report an emergency, even if the person was unaware of the screen saver password.

[0031] Optionally, the types of calls that are enabled when the computing device 12 is in the locked mode includes internal calls. Thus, if the user of the computing device 12 attempts to contact the user of the computing device 16 of Fig. 1, connectivity could be established while maintaining the computing device in the locked mode. However, a call to a telephone beyond the firewall 32 could not be completed until the prescribed authorization process is completed and the computing device is returned to its normal operation mode.

[0032] In step 62, the computing device 12 is in the normal operation mode, but monitors the system to determine if the preset conditions are established for switching the computing device to the locked mode. In Fig. 2, the security module 58 monitors idle time to determine when the preconfigured idle-time period has been exceeded. If in the determination step 64 a preset condition is recognized, the computing device 12 is switching to the locked mode in step 66. As previously noted, this disables access to the local memory 48, removes potentially sensitive subject matter from the screen monitor 52, and restricts use of the TOL 54.

[0033] In step 68, the system monitors for the authorization condition that triggers a switch from the locked mode to the normal operation mode. If in the determination step 70 the authorization condition is recognized, e.g., a password is entered, the switch to the normal operation mode is executed at step 72 and the process returns to the monitoring step 62.

[0034] In step 74, a TOL access is recognized before the authorization condition is established. If in step 76 the TOL access is determined to be an attempt to initiate an outgoing call, the determination step 78 ascertains whether the attempted outgoing call is of a call type that was designated as being accessible when the computing device 12 is in the locked mode. As previously noted, the computing device is preferably configured to allow outgoing emergency calls to be completed when the computing device is in the locked mode. A determination at step 78 that the outgoing call is permissible results in the initiation of connectivity at step 80. With connectivity for the selected outgoing call initiated, the process returns to the step 68 of monitoring for the authorization condition that is necessary to return the computing device to the normal operation mode. On the other hand, a determination at step 78 that the outgoing call is not identified as a permissible outgoing call results in a denial of access at step 82 and a return to the monitoring step 68.

[0035] Returning to step 76 of Fig. 3, a determination that the TOL access is an incoming call results in a call notification at step 84. For example, the recognition of the call may allow the TOL 54 to occupy the monitor screen 52 in a minimized state. Connectivity may be initiated at step 80, but the window may be restricted to its minimized state. Moreover, the user is restricted from opening any other programs or windows. In this secure condition, the computing device 12 is locked in the TOL window and the security of the data and outgoing call capabilities of the computing device is not compromised. However, the process is returned to step 68 to allow an authorized user to return the computing device to the normal operation mode by entering the password or other authentication item.

[0036] While the process flow of Fig. 3 has been described primarily with respect to telecommunications, this is not critical. The method may be used in connec-

tion with other communication environments. For example, email notification and screen saver capabilities can be integrated in the manner described with reference to Figs. 2 and 3.

Claims

1. A method of maintaining security for a computing device connected to a network to receive incoming communications comprising steps of:

   configuring said computing device such that said computing device switches from an operative mode to a locked mode in response to detection of a preset condition and switches from said locked mode to said operative mode in response to detection of a preset authorization condition, said locked mode establishing a security condition with respect to data access capabilities and communication access capabilities of said computing device;
   enabling notification at said computing device when an incoming communication is directed to said computing device; and
   enabling access to said communication access capabilities of said computing device in response to detecting said notification that said incoming communication is directed to said computing device, including providing access to handling said incoming communication while maintaining said security condition with respect to said data access capabilities until said detection of said preset authorization condition.

2. The method of claim 1 wherein said step of configuring said computing device includes setting parameters of a password protected screen saver that is responsive to said detection of said preset condition, including setting a password such that input of said password satisfies said preset authorization condition.

3. The method of claim 1 wherein said step of enabling access to said communication access capabilities includes limiting said access, to handling said incoming communication, such that initiation of outgoing communications is denied in the absence of said preset authorization condition.

4. The method of claim 3 wherein said step of configuring said computing device includes setting operational parameters of a telephony-over-LAN (TOL) application, said incoming communication being a telephone call that includes at least one of voice and video information.

5. The method of claim 4 further comprising a step of installing said TOL application in said computing device such that said TOL application is integrated with a screen saver that is configurable with respect to selection of said preset authorization condition, said step of configuring said computing device including selecting operational parameters of said screen saver.

6. The method of claim 4 further comprising steps of installing said TOL application and installing a screen saver application in said computing device, said TOL and screen saver applications being operationally compatible with respect to switching said communication access capabilities of said computing device from said locked mode to said operative mode while maintaining said data access capabilities in said locked mode when said notification is detected separately from said preset authorization condition.

7. The method of claim 1 wherein said step of configuring said computing device includes defining limitations on utilizing said communication access capabilities when said computing device is in said locked mode, including identifying limited types of outgoing telephone calls that can be initiated in the absence of detecting said preset authorization condition.

8. The method of claim 1 wherein said step of configuring said computing device includes setting operational parameters of an email application, said incoming communication being an email message.

9. In a computing device connected to a network to receive incoming communications, a security system comprising:

   screen saver means for selectively establishing a security condition with respect to disabling data access capabilities and communication access capabilities of said computing device, said screen saver means having a locked mode and an operative mode, said screen saver means being in said locked mode when said security condition is established;
   means for recognizing a predefined authorization sequence to override said locked mode of said screen saver means, thereby switching said screen saver means from said locked mode to said operative mode in which said data access and communication access capabilities are enabled; and
   means for enabling a first set of communication access capabilities of said computing device in response to detection of an incoming communication with said screen saver means in said locked mode, said first set including enabling

handling of said incoming communication while said screen saver means remains in said locked mode with respect to said data access capabilities and with respect to a second set of said communication access capabilities.

10. The security system of claim 9 wherein said communication access capabilities include telephone means for enabling a telephone connection.

11. The security system of claim 10 wherein said first set of said communication access capabilities relates to connectivity of said telephone means to receive incoming calls and to initiate specified types of outgoing calls.

12. The security system of claim 9 wherein said screen saver means and said means for enabling are integrated in computer software.

13. The security system of claim 9 wherein said means for enabling includes configurable memory for defining said first and second sets of communication access capabilities.

14. The security system of claim 13 wherein said screen saver means is configurable software having password protection, said means for recognizing being a program module for identifying a specified password.

15. A method of maintaining security for a computing device connected to a network to handle incoming and outgoing telephone calls having at least one of voice and video information, said method comprising steps of:

timing periods of inactivity by said computing device;
automatically switching said computing device from an operative mode to a screensaver mode when a period of inactivity exceeds a predetermined time period, including securing access to data and outgoing call capabilities of said computing device while enabling notification of an incoming call;
monitoring a communications line connecting said communication device to said network to detect incoming calls;
providing a notification at said computing device in response to detecting an incoming call;
enabling handling of said incoming call while maintaining said computing device in said screensaver mode with respect to data and outgoing call capabilities; and
switching said computing device from said screensaver mode to said operative mode in response to input of a password to said computing device.

16. The method of claim 15 wherein said step of securing access to data and outgoing call capabilities includes freeing said computing device to initiate preselected types of outgoing calls while said computing device is in said screensaver mode.

17. The method of claim 16 wherein said step of freeing said computing device includes enabling emergency calls when said computing device is in said screensaver mode.

18. The method of claim 15 wherein each of said steps of said method is executed in computer software.

19. The method of claim 15 wherein said step of providing said notification includes triggering an image on a monitor screen of said computing device.

20. A method of maintaining security for a computing device connected to a network to receive incoming communications comprising steps of:

enabling screen saver capability for protecting data accessible via said computing device;
establishing an idle time threshold for switching said screen saver capability from a normal operation mode to a locked mode in which said data is protected from access;
monitoring data accesses and communication sessions involving said computing device to detect periods of inactivity exceeding said idle time threshold;
triggering a switch from said normal operation mode to said locked mode upon detecting an absence of a data access and a communication session for a period exceeding said idle time threshold; and
returning said computing device to said normal operation mode upon detecting a preset authorization condition.

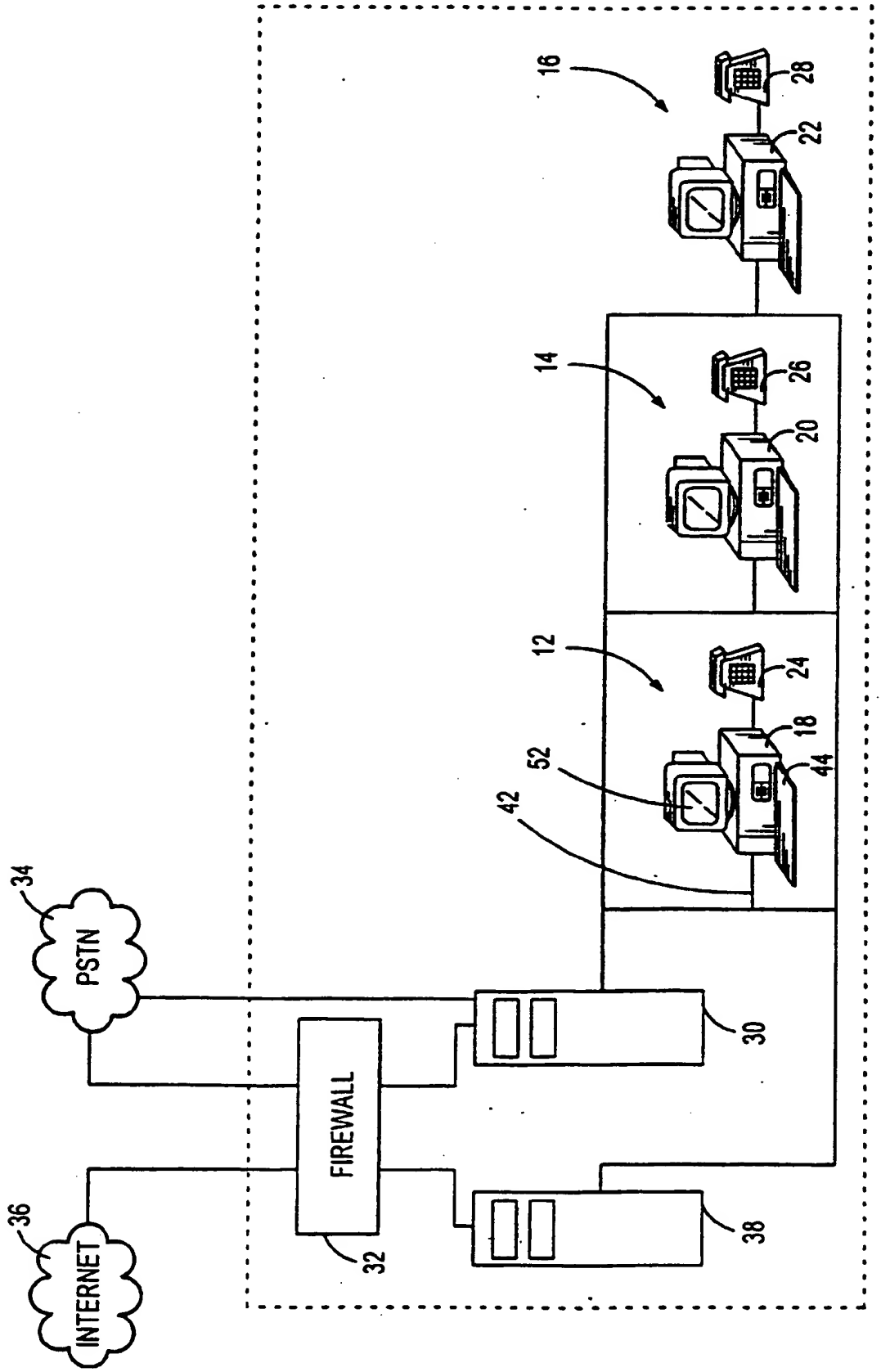

FIG. 1

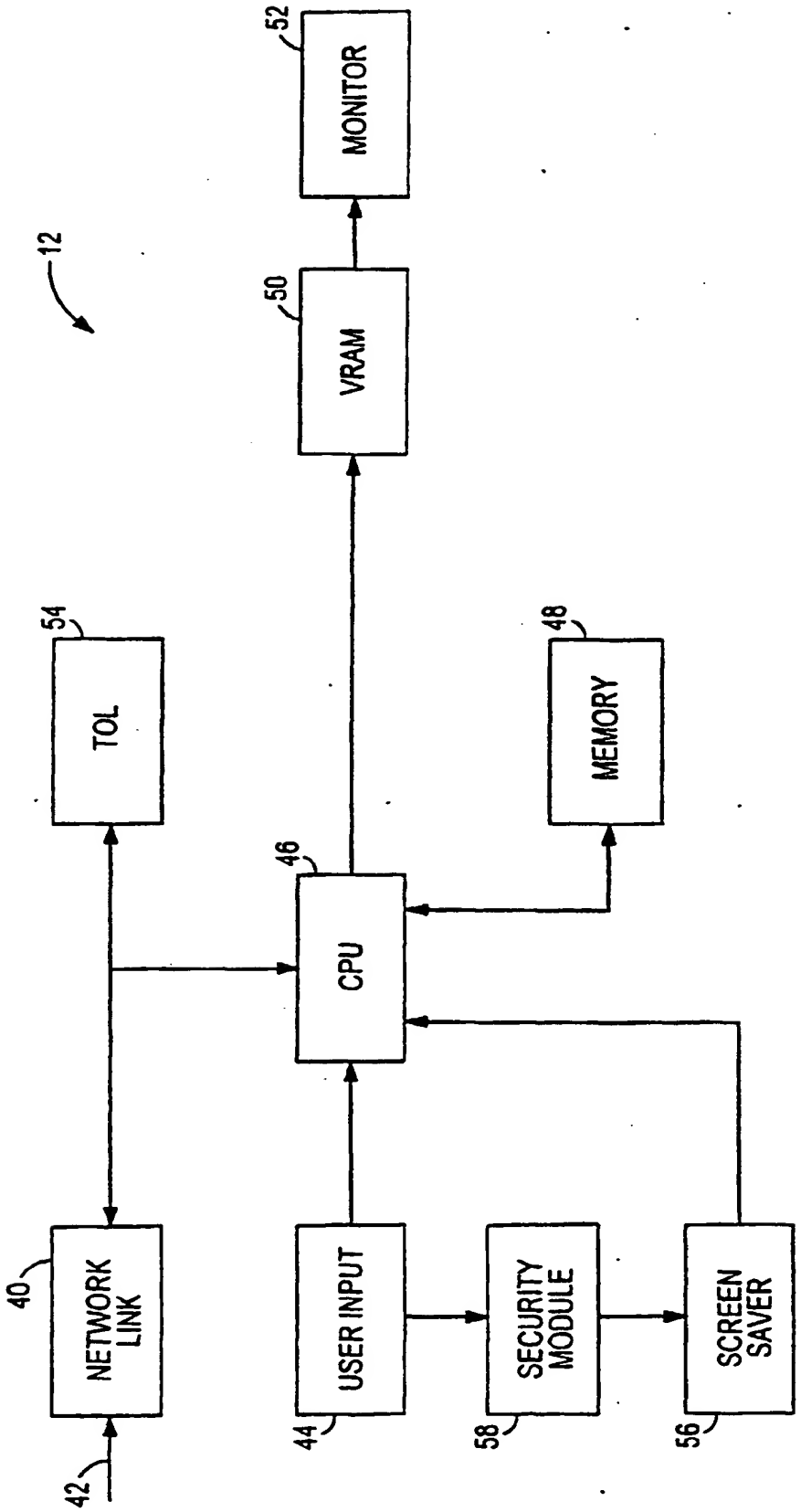

FIG. 2

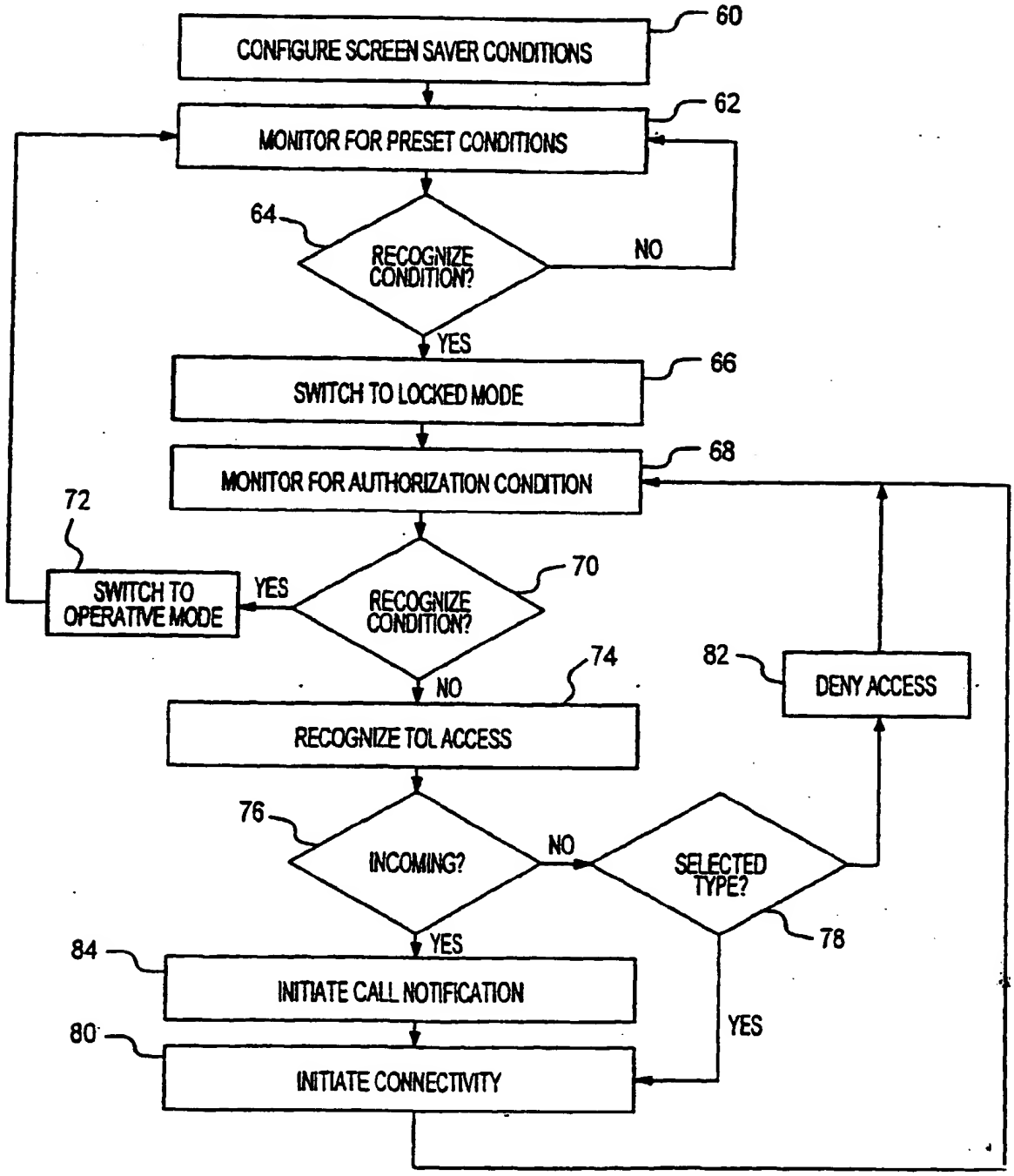

FIG. 3